(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－279727
（P2002－279727A）
(43)公開日　平成14年９月27日(2002.9.27)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	５Ｃ０５３
20/12		20/12		５Ｄ０４４
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00	６４１	５Ｊ１０４
Ｈ０４Ｎ　5/91		Ｈ０４Ｎ　5/91	Ｐ	

審査請求　未請求　請求項の数25　ＯＬ　（全 13 頁）

(21)出願番号　特願2001－76723(P2001－76723)

(22)出願日　平成13年３月16日(2001.3.16)

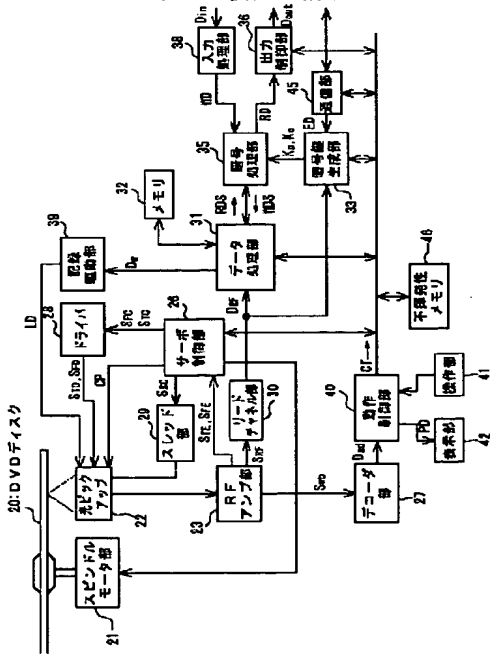
(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　郡　照彦
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100090376
弁理士　山口　邦夫　（外１名）

最終頁に続く

(54)【発明の名称】　信号記録媒体とコンテンツ信号生成装置及びコンテンツ信号再生方法とコンテンツ信号再生装置

(57)【要約】
【課題】コンテンツ信号の再生の制限を容易に可能とする。
【解決手段】ディスク２０に、再生を制限する再生制限機能を働かせるか否かを示す制御信号を付加したコンテンツ信号を記録する。再生時に暗号鍵生成部３３で再生制限機能を働かせることを示す制御信号が付加されていることを判別したときには、再生許可条件を満たすか否かを判別する。再生許可条件は、ディスク２０から読み出す。また、ディスク２０に記録されていないときには通信部４５を介して入手する。再生許可条件を満たすときにのみ、正しい暗号鍵Kpを暗号処理部３５に供給する。暗号処理部３５では、暗号化されてディスク２０に記録されているコンテンツ信号を暗号鍵Kpで復号化して、正しく復号化されたコンテンツ信号を出力制御部３６から出力する。

ディスク装置の構成



1

【特許請求の範囲】

【請求項１】　コンテンツ信号に、該コンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号を付加し、
前記制御信号を付加したコンテンツ信号を記録したことを特徴とする信号記録媒体。

【請求項２】　前記コンテンツ信号には、前記再生制限機能を働かせたときに前記コンテンツ信号の再生許可条件を示す条件信号も付加して記録したことを特徴とする請求項１記載の信号記録媒体。

【請求項３】　前記コンテンツ信号は、
前記情報信号と予め設定された暗号鍵とに基づいて生成した新たな暗号鍵を用いて暗号化した信号であることを特徴とする請求項１記載の信号記録媒体。

【請求項４】　前記コンテンツ信号は、
前記情報信号と予め設定された暗号鍵と前記条件信号に基づいて生成した新たな暗号鍵を用いて暗号化した信号であることを特徴とする請求項２記載の信号記録媒体。

【請求項５】　前記コンテンツ信号は、復号化が正常に完了したか否かを判別可能とする検査データを付加した信号であることを特徴とする請求項１記載の信号記録媒体。

【請求項６】　コンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号を供給して、コンテンツ信号の再生制限動作を設定する信号生成制御手段と、
前記コンテンツ信号に前記信号生成制御手段から供給された情報信号を付加して、コンテンツ流通用のコンテンツ信号を生成する信号生成手段とを有することを特徴とするコンテンツ信号生成装置。

【請求項７】　前記信号生成制御手段では、前記再生制限機能を働かせたときに前記コンテンツ信号の再生許可条件を示す条件信号の生成も行うものとし、
前記信号生成手段では、前記条件信号も付加して前記コンテンツ流通用のコンテンツ信号を生成することを特徴とする請求項６記載のコンテンツ信号生成装置。

【請求項８】　コンテンツ信号の暗号化を行う暗号化手段と、
前記暗号化手段で前記コンテンツ信号の暗号化を行う際に用いる暗号鍵を、前記情報信号と予め設定された暗号鍵とに基づいて生成する暗号鍵生成手段とを有することを特徴とする請求項６記載のコンテンツ信号生成装置。

【請求項９】　コンテンツ信号の暗号化を行う暗号化手段と、
前記暗号化手段で前記コンテンツ信号の暗号化を行う際に用いる暗号鍵を、前記情報信号と予め設定された暗号鍵と前記条件信号に基づいて生成する暗号鍵生成手段とを有することを特徴とする請求項７記載のコンテンツ信号生成装置。

【請求項１０】　復号化が正常に完了したか否かを判別

2

可能とする検査データを前記コンテンツ信号に付加する付加手段を有することを特徴とする請求項６記載のコンテンツ信号生成装置。

【請求項１１】　コンテンツ信号を再生する際に、
前記コンテンツ信号が、前記コンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号を有しているか否かを判別するものとし、
前記情報信号を有していると判別されたときには、前記コンテンツ信号の再生を許可する再生許可条件を満たしたときに、前記コンテンツ信号を出力することを特徴とするコンテンツ信号再生方法。

【請求項１２】　前記コンテンツ信号が、前記再生制限機能を働かせたときに前記コンテンツ信号の再生許可条件を示す条件信号を有しているとき、
前記条件信号で示された条件を満たしたときに、前記コンテンツ信号を出力することを特徴とする請求項１１記載のコンテンツ信号再生方法。

【請求項１３】　前記コンテンツ信号が、前記再生制限機能を働かせたときに前記コンテンツ信号の再生許可条件を示す条件信号を有していないとき、
前記再生許可条件の入手を行い、入手した再生許可条件を満たしたときに、前記コンテンツ信号を出力することを特徴とする請求項１１記載のコンテンツ信号再生方法。

【請求項１４】　前記再生許可条件は、通信手段を介して、あるいは予め再生許可条件を記憶した条件記憶手段から入手することを特徴とする請求項１３記載のコンテンツ信号再生方法。

【請求項１５】　前記再生許可条件を満たしたときには、前記制限信号と前記コンテンツ信号が有する鍵情報に基づいて暗号鍵を生成し、
前記暗号鍵を用いて復号化が行われたコンテンツ信号を出力することを特徴とする請求項１１記載のコンテンツ信号再生方法。

【請求項１６】　前記再生許可条件を満たしたときには、前記制限信号と前記コンテンツ信号が有する鍵情報と前記条件信号に基づいて暗号鍵を生成し、
前記暗号鍵を用いて復号化が行われたコンテンツ信号を出力することを特徴とする請求項１２記載のコンテンツ信号再生方法。

【請求項１７】　前記コンテンツ信号は、暗号化された信号であると共に復号化が正常に完了したか否かを判別可能とする検査データを付加した信号である場合、
前記復号化を行い前記検査データによって復号化が正常に完了したと判別されたときに、前記コンテンツ信号を出力することを特徴とする請求項１１記載のコンテンツ信号再生方法。

【請求項１８】　前記検査データによって復号化が正常に完了したと判別されないときには、コンテンツ信号の出力を行うことができないことを通知することを特徴と

する請求項１７記載のコンテンツ信号再生方法。

【請求項１９】　コンテンツ信号が、前記コンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号を有しているか否かを判別すると共に、前記情報信号を有していると判別されたときに、前記コンテンツ信号の再生を許可する再生許可条件を満たしている場合、前記コンテンツ信号を正しく出力可能とする設定信号の生成を行う設定信号生成手段と、

前記設定信号生成手段からの設定信号を用いて前記コンテンツ信号の出力処理を行う出力処理手段とを有することを特徴とするコンテンツ信号再生装置。

【請求項２０】　前記設定信号生成手段では、前記コンテンツ信号から前記再生許可条件を示す条件信号を抽出し、前記条件信号で示された再生許可条件を満たしたときに、前記設定信号を出力することを特徴とする請求項１９記載のコンテンツ信号再生装置。

【請求項２１】　通信手段を有し、

前記設定信号生成手段では、前記コンテンツ信号から前記条件信号を抽出できないときに、前記通信手段を介して前記条件信号を入手することを特徴とする請求項２０記載のコンテンツ信号再生装置。

【請求項２２】　条件信号を記憶した記憶手段を予め設けるものとし、

前記設定信号生成手段では、前記コンテンツ信号から前記条件信号を抽出できないときに、前記記憶手段から前記条件信号を入手することを特徴とする請求項２０記載のコンテンツ信号再生装置。

【請求項２３】　前記設定信号生成手段では、前記条件信号で示された条件を満たしたときに、コンテンツ信号を正しく復号化する暗号鍵を設定信号として出力するものとし、

前記出力処理手段では、前記コンテンツ信号の出力の際に前記暗号鍵を用いた復号化を行うことを特徴とする請求項１９記載のコンテンツ信号再生装置。

【請求項２４】　前記コンテンツ信号に復号化が正常に完了したか否かを判別可能とする検査データが付加されている場合、

前記出力処理手段では、前記復号化を行い前記検査データによって復号化が正常に完了したと判別されたときに、復号化された前記コンテンツ信号を出力することを特徴とする請求項２３記載のコンテンツ信号再生装置。

【請求項２５】　動作状態を通知する通知手段を有し、

前記出力処理手段において、前記検査データによって復号化が正常に完了したと判別されないときには、前記通知手段によってコンテンツ信号の出力を行うことができないことを通知することを特徴とする請求項２４記載のコンテンツ信号再生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、記録媒体とコンテンツ信号生成装置及びコンテンツ信号再生方法とコンテンツ信号再生装置に関する。詳しくは、コンテンツ信号に再生を制限する再生制限機能を働かせるか否かを示す制御信号を付加するものとし、再生制限機能が働いているときには、再生許可条件を満たす場合にのみコンテンツ信号の再生を可能とすることで、コンテンツ信号の再生を制限可能とするものである。

【０００２】

【従来の技術】近年、画像・音声・テキストなどの様々なコンテンツの情報をディジタル化し統合的に取り扱うことが可能となりつつある。このように種々のコンテンツをディジタル化して配布する場合、例えば音楽や映画等が記録された記録媒体を販売する場合、記録媒体にはコンテンツがディジタル信号として記録されていることから、完全な複製を容易かつ無尽蔵に作成できてしまう。これは利用者にとっては大きな利点であるが、著作物を提供する側にとっては権利保護の面で問題となる。したがって、ディジタル化されたコンテンツを配布する際には、ディジタル情報としての特徴を損なわずにしかも著作権を保護できるような仕組みが実用化されている。

【０００３】この著作権保護の仕組みとして、オーディオコンテンツに対しては、例えばディジタルオーディオテープ（ＤＡＴ）やミニディスク（ＭＤ）において、ＳＣＭＳ(Serial Copy Management System)と呼ばれるコピー制御ビットを、コンテンツ信号に設けることが行われている。このコピー制御ビットでは、コピー許可されているかコピー禁止とされているかあるいはコピーされたものであるかなどが示されており、このコピー制御ビットによって、コピー動作が制御される。またビデオコンテンツに対しては、例えば民生用ディジタルビデオ規格（ＤＶＣ）やＤＶＤ－ＶＲ(Video Recording)において、ＣＧＭＳ(Copy Generation Management System)と呼ばれるコピー制御ビットが設けられている。このコピー制御ビットによって、コピー許可、１世代だけコピー許可、コピー禁止あるいはコピーされたものであるかが示されており、このコピー制御ビットによってＳＣＭＳと同様にコピー動作が制御されている。さらに、ＤＶＤ－ＡＲ(Audio Recording)の規格化で検討されているＣＱＲＴと呼ばれるコピー制御情報(CCI:Copy ControlInformation)では、コピーを許可するか否かなどの情報だけでなく、オーディオの品質を制御する情報や関連するコンテンツ信号のコピーを許可するか否かの情報等も示されて、コピー動作をさらに詳細に制御する方法が提案されている。

【０００４】

【発明が解決しようとする課題】ところで、ＳＣＭＣやＣＧＭＳ等のコピー制御は、コンテンツ信号のコピーを許可するか否かを制御するものであることから、コンテンツ信号の再生回数や再生期限等を制限することができ

ない。このため、市場に広く普及している記録媒体を利用してコンテンツの提供を行う際に、例えば再生回数や再生期限を制限してプレビューサービス等を行うものとしたり、再生回数や再生期限を制御することでコンテンツを安価に提供するなどのサービスを行うことはできない。そこで、この発明では、コンテンツ信号の再生の制限を容易に行うことができる、信号記録媒体とコンテンツ信号生成装置及びコンテンツ信号再生方法とコンテンツ信号再生装置を提供するものである。

【０００５】

【課題を解決するための手段】この発明に係る信号記録媒体は、コンテンツ信号に、該コンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号を付加し、制御信号を付加したコンテンツ信号を記録したものである。

【０００６】コンテンツ信号生成装置は、コンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号を供給する信号生成制御手段と、コンテンツ信号に信号生成制御手段から供給された情報信号を付加して、コンテンツ流通用のコンテンツ信号を生成する信号生成手段とを有するものである。さらに、コンテンツ信号の暗号化を行う暗号化手段と、暗号化手段でコンテンツ信号の暗号化を行う際に用いる暗号鍵を、情報信号と予め設定された暗号鍵とに基づいて生成する暗号鍵生成手段とを有するものである。また、復号化が正常に完了したか否かを判別可能とする検査データをコンテンツ信号に付加する付加手段を有するものである。

【０００７】コンテンツ信号再生方法は、コンテンツ信号を再生する際に、コンテンツ信号がコンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号を有しているか否かを判別するものとし、情報信号を有していると判別されたときには、コンテンツ信号の再生を許可する再生許可条件を満たしたときに、コンテンツ信号を出力するものである。

【０００８】コンテンツ信号再生装置は、コンテンツ信号がコンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号を有しているか否かを判別すると共に、情報信号を有していると判別されたときに、コンテンツ信号の再生を許可する再生許可条件を満たしている場合、コンテンツ信号の出力を可能とする設定信号を出力する設定信号生成手段と、設定信号生成手段からの制御信号に基づきコンテンツ信号の出力処理を行う出力処理手段とを有するものである。また通信手段を有し、設定信号生成手段では、コンテンツ信号から条件信号を抽出できないときに、通信手段を介して条件信号を入手するものである。さらに、条件信号を記憶した記憶手段を予め設けるものとし、設定信号生成手段では、コンテンツ信号から条件信号を抽出できないときに、記憶手段から条件信号を入手するものである。また、動作状態を通知する通知手段を有し、出力処理手段

において、検査データによって復号化が正常に完了したと判別されないときには、通知手段によってコンテンツ信号の出力を行うことができないことを通知するものである。

【０００９】この発明においては、コンテンツ信号に、このコンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号が付加されると共に、この情報信号と予め設定された暗号鍵とに基づいて生成した新たな暗号鍵を用いてコンテンツ信号が暗号化される。また、再生制限機能を働かせたときにコンテンツ信号の再生許可条件を示す条件信号も付加されると共に、この条件信号も用いて生成した新たな暗号鍵を用いてコンテンツ信号が暗号化される。この制御信号や条件信号が付加されている暗号化されたコンテンツ信号が、コンテンツ流通用の信号として記録媒体に記録されるあるいは通信回線を介して配信される。さらに、コンテンツ信号には、復号化が正常に完了したか否かを判別可能とする検査データが付加される。

【００１０】また、コンテンツ信号の再生では、コンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号を有しているか否かが判別される。ここで、情報信号を有していると判別されたとき、コンテンツ信号が有している再生許可条件や通信回線等を介して入手した再生許可条件を満たしている場合には、情報信号と予め設定された暗号鍵とに基づいて生成した新たな暗号鍵を用いてコンテンツ信号が復号化される。また、コンテンツ信号が再生許可条件を有しているときには、この再生許可条件を示す条件信号も用いて生成した新たな暗号鍵を用いてコンテンツ信号が復号化される。さらに、復号化が正常に完了したか否かを判別可能とする検査データがコンテンツ信号に付加されている場合、検査データによって復号化が正常に完了したと判別されたときに、コンテンツ信号が出力されると共に、検査データによって復号化が正常に完了したと判別されないときには、コンテンツ信号の出力を行うことができないことが通知される。

【００１１】

【発明の実施の形態】以下、図を参照しながら、この発明の実施の一形態について説明する。図１は例えばＤＶＤオーディオにおけるコンテンツの構造を示している。コンテンツは、ナビゲーション情報とメタデータ及びエレメンタリーストリームで構成される。ナビゲーション情報は、コンテンツの目次やＧＵＩ等で構成される。またメタデータは、演奏者名や歌詞などのようにコンテンツに付随した付加情報、及びコピー制御情報ＣＣＩで通常構成される。また、エレメンタリーストリームは、リニアＰＣＭのオーディオデータやＭＰＥＧ(Moving Picture Experts Group)オーディオ規格に対応したオーディオデータ等で構成される。ここで、本発明では、コンテンツ信号の再生を制限する再生制限機能を働かせるか否

かを示す制御信号である再生許可ビット(ＰＢＰ:Playback Permission bit)を、メタデータに付加する。さらに、このメタデータには、再生許可条件を示す条件信号である再生条件情報(ＰＢＣ:Playback Condition information)を設けることも可能とする。

【００１２】図２は、コンテンツ信号の信号記録媒体であるＤＶＤ(Digital Versatile Disc)のディスク構成を示している。ディスクの最内周側にはリードイン領域が設けられており、ディスクの物理的な仕様やコンテンツ供給者の情報等が示される。このコンテンツ供給者の情報は、後述するデータ領域に暗号化されて記録されているコンテンツを復号化するために用いるディスクキーを有している。また、リードイン領域には、ＢＣＡ(Burst Cutting Area)を設けて、ディスク固有の情報、例えばディスクのシリアルＩＤのようなデータをレーザカッターによってバーコード状に記録することが可能とされている。リードイン領域の外周側はデータ領域とされており、このデータ領域にコンテンツ信号が記録される。データ領域の外周側にはデータ領域の終了を示すリードアウト領域が設けられており、光ビームの照射位置が、リードイン領域からリードアウト領域の範囲内で移動可能とされる。

【００１３】また、ＤＶＤ規格では、追記や書き換え可能なディスクである場合、ＵＤＦ(Universal Disk Format)のファイルシステムが用いられる。また、再生専用のディスクの場合には、ＣＤ－ＲＯＭの規格として用いられているＩＳＯ(International Organization for Standardization)９６６０とＵＤＦ(Universal Disk Format)の両方の規格に対応するため、「ＵＤＦ　Ｂｒｉｄｇｅ」と呼ばれるファイルシステムが用いられている。

【００１４】ここで、コンテンツ信号がオーディオのコンテンツである場合には、上述のファイルシステムにおいて、コンテンツ信号がＡＵＤＩＯ－ＴＳのディレクトリ構成とされてディスクに記録される。例えば目次等がＡＵＤＩＯ－ＴＳ．ＩＦＯのデータ、コンテンツに付随した付加情報がＡＴＳ（オーディオタイトルセット）．ＩＦＯのデータ、オーディオデータがＡＴＳ．ＡＯＢのデータとされる。また、コピー制御情報ＣＣＩや再生許可ビットＰＢＰ、再生条件情報ＰＢＣは、セクタ単位で記録されたコンテンツデータのセクタヘッダ部に設けるものとしたり、ファイル化してデータ領域に記録する。なお、コピー制御情報ＣＣＩや再生許可ビットＰＢＰ、再生条件情報ＰＢＣの記録位置は上述の位置に限られるものではない。

【００１５】ここで、ＡＵＤＩＯ－ＴＳのディレクトリの情報をディスクに記録して再生専用のディスクを生成する場合には、ＣＳＳ(Content Scrambling System)の認証方法を用いるものとして、ＣＰＰＭ(Content Protection for Prerecorded Media)と呼ばれる暗号方式でコンテンツの信号の暗号化を行い、暗号化されたコンテンツ信号を用いてディスクを生成する。

【００１６】図３はコンテンツ信号生成装置の構成を示す概略図である。信号生成部１１では、信号生成制御部１３から供給された制御信号ＭＣＳに基づいて、記憶装置１２に記憶されているオーディオデータやナビゲーション情報及びコンテンツに付随した付加情報を読み出しコンテンツを構成する信号ＣＳａを生成する。また、コピー制限や再生制限を行う場合には、信号生成制御部１３からコピー制御情報ＣＣＩや再生許可ビットＰＢＰを信号生成部１１に供給して、コンテンツを構成する信号ＣＳａ内にこれらの信号を付加する。さらに、再生制限機能を動作させた場合の再生許可条件も含ませる場合には、この再生許可条件を示す再生条件情報ＰＢＣも信号生成部１１に供給する。このようにして信号生成部１１で生成された信号ＣＳａは暗号処理部１４に供給する。

【００１７】信号生成制御部１３では、上述したように信号生成部１１に対して制御信号ＭＣＳや各種の情報等を供給すると共に、信号生成部１１で生成された信号ＣＳａの暗号化に用いる暗号鍵を生成するために再生許可ビットＰＢＰや再生条件情報ＰＢＣを暗号鍵生成部１５に供給する。また、信号変換部１６には、リードイン領域に記録するＴＯＣ(Table Of Contents)情報ＴＣや、信号変換動作を制御する制御信号ＭＣＦを供給する。

【００１８】ここで、ＣＰＰＭの暗号化を行う場合、暗号鍵生成部１５では、従来のようにディスク単位の暗号鍵Keを暗号処理部１４に供給するだけでなく、コンテンツ信号の再生制限機能を利用するときには、暗号鍵Ke用いるだけでなく供給された再生許可ビットＰＢＰを用いた暗号化を行う。例えば、再生許可ビットＰＢＰから暗号鍵Kpbpを生成して、この暗号鍵Kpbpと従来より用いられているディスク単位の暗号鍵Keとから新たな暗号鍵Kpを生成して、この暗号鍵Kpを暗号処理部１４に供給する。

【００１９】この新たな暗号鍵Ｋｐの生成では、例えば再生許可ビットＰＢＰから予め定められたアルゴリズムに基づいて暗号鍵Kpbpを生成して、この暗号鍵Kpbpと暗号鍵Keを用いて所定の演算を行い暗号鍵Kpを生成する。このとき、暗号鍵Kpの鍵長を暗号鍵Keと等しくすれば、従来の暗号化方式と鍵長の互換性を保つことができることから、再生許可ビットＰＢＰを追加するために必要な変更点を少なくできる。また、新たな暗号鍵Kpの鍵長を暗号鍵Keよりも長くすることにより暗号強度を高めることも容易に行うことができる。また、暗号鍵Kpの生成に用いたディスク単位の暗号鍵Keを、例えばメーカー毎に割り当てられたマスター鍵Kmで暗号化して暗号鍵Ke'として信号変換部１６に供給する。

【００２０】また、再生条件情報ＰＢＣも用いてコンテンツ信号を生成する場合には、この再生条件情報ＰＢＣを暗号鍵生成部１５に供給して再生条件情報ＰＢＣに基づく暗号鍵Kpbcを生成し、暗号鍵Ke，Kpbpだけでな

く暗号鍵Kpbcも用いて新たな暗号鍵Kpの生成を行う。

【００２１】暗号処理部１４では、暗号鍵生成部１５から供給された暗号鍵Kpを用いて信号ＣＳaの暗号化を行い信号ＣＳbとして信号変換部１６に供給する。なお、暗号鍵生成部１５から、暗号処理部１４に対して暗号鍵Keや暗号鍵Kpbp，Kpbcを別個に供給して、暗号処理部１４では、それぞれの暗号鍵を用いた暗号化を繰り返し行い、このようにして得られた信号を信号変換部１６に供給するものとしても良い。しかし、新たな暗号鍵Kpを生成して暗号化を行うものとすれば、新たな暗号鍵の生成処理を追加するだけで、従来と同様に暗号化処理を行うことができるので、再生制限機能を設けるものとしたときの変更部分を少なくできる。なお、暗号処理部１４では、信号ＣＳaを暗号化して信号ＣＳbを生成する際に、信号ＣＳbから再生許可ビットＰＢＰや再生条件情報ＰＢＣを分離可能に暗号化する。

【００２２】信号変換部１６では、暗号化された信号ＣＳbと信号生成制御部１３から供給されたＴＯＣ情報及び暗号鍵Ke’などを用いてコンテンツ信号を生成すると共に、このコンテンツ信号を記録媒体に応じたフォーマットに変換して記録信号ＷＡを生成する。この記録信号ＷＡを用いてマスターディスクを生成し、このマスターディスクを用いてスタンパーを形成することで、このスタンパーを用いてコンテンツ信号の再生制限を行うことができるＤＶＤディスクを簡単かつ容易に生成できる。

【００２３】追記あるいは書き換え可能なＤＶＤディスクでは、コンテンツ信号の記録機能を有するディスク装置によって、例えばＣＰＲＭ(Content Protection for Recordable Media)と呼ばれる暗号方式で暗号化を行い、暗号化された信号をディスクに記録する。ここで、コンテンツ信号を記録する場合、ディスクには再生専用ディスクのようにディスク単位の暗号鍵Keがマスター鍵Kmで暗号化されて記録されているわけではない。このため、例えば上述のリードイン領域に設けられたＢＣＡに記録されているディスク固有の情報を利用して暗号鍵Keを生成すると共に、この暗号鍵Keを用いて暗号化を行う。あるいは、記録された楽曲を曲単位で保護出来るようにトラック毎に生成した暗号鍵Ktも用いた暗号化を行う。さらに、再生制御を行うときには、上述のように再生許可ビットＰＢＰも用いて新たな暗号鍵Kpを生成し、この暗号鍵Kpを用いて暗号化を行う。

【００２４】また、上述のＣＰＲＭの暗号化では、再生許可ビットＰＢＰから生成した暗号鍵Kpbpを用いて暗号鍵Kpを生成すると共に暗号鍵Kpを用いてして暗号化を行うものとしたが、再生許可条件を設定してコンテンツの再生を制限する場合には、再生許可条件を示す再生条件情報ＰＢＣをディスクに記録すると共に、この再生条件情報ＰＢＣに基づく暗号鍵Kpbcを生成して、暗号鍵Ke，Kpbpだけでなく暗号鍵Kpbcも用いて新たな暗号鍵Kpの生成を行う。

【００２５】次に、上述のように再生許可ビットＰＢＰや再生条件情報ＰＢＣも用いたコンテンツ信号の記録再生を行うディスク装置の構成を図４に示す。ＤＶＤディスク２０は、スピンドルモータ部２１によって所定の速度で回転される。なお、スピンドルモータ部２１は、後述するサーボ制御部２６からのスピンドル制御信号Sspに基づいて、ＤＶＤディスク２０の回転速度が所定の速度となるように駆動される。

【００２６】ＤＶＤディスク２０には、光ピックアップ２２から光量をコントロールした光ビームが照射される。ＤＶＤディスク２０で反射された光ビームは、光ピックアップ２２の光検出部（図示せず）に照射される。光検出部では反射された光ビームに基づき光電変換や電流電圧変換を行い、反射された光ビームの光量に応じた信号レベルの電圧信号を生成してＲＦアンプ部２３に供給する。

【００２７】ＲＦアンプ部２３では、光ピックアップ２２からの電圧信号を用いて読出信号SRFを生成してリードチャネル部３０に供給する。また、トラッキング誤差信号STE、フォーカス誤差信号SFEを生成して、サーボ制御部２６に供給する。さらに、ディスク装置が例えばＤＶＤ＋ＲＷに対応するものであるときには、ウォーブル信号Swbが生成されてデコーダ部２７に供給される。

【００２８】サーボ制御部２６では、供給されたフォーカス誤差信号SFEに基づき、レーザ光の焦点位置がＤＶＤディスク２０の記録層の位置となるように光ピックアップ２２の対物レンズ（図示せず）を制御するためのフォーカス制御信号SFCを生成してドライバ２８に供給する。また、供給されたトラッキング誤差信号STEに基づき、光ビームの照射位置が所望のトラックの中央位置となるように光ピックアップ２２の対物レンズを制御するためのトラッキング制御信号STCを生成してドライバ２８に供給する。

【００２９】ドライバ２８では、フォーカス制御信号SFCに基づいてフォーカス駆動信号SFDを生成すると共に、トラッキング制御信号STCに基づいてトラッキング駆動信号STDを生成する。この生成されたフォーカス駆動信号SFD及びトラッキング駆動信号STDを光ピックアップ２２のアクチュエータ（図示せず）に供給することで、光ビームが所望のトラックの中央位置で焦点を結ぶように対物レンズを制御する。

【００３０】また、サーボ制御部２６では、レーザ光の照射位置がトラッキング制御範囲を越えないように、光ピックアップ２２をＤＶＤディスク２０の径方向に移動させるためのスレッド制御信号SSCを生成してスレッド部２９に供給する。スレッド部２９では、このスレッド制御信号SSCに基づきスレッドモータを駆動して光ピックアップ２２をＤＶＤディスク２０の径方向に移動させる。また、レーザ出力制御信号ＣＰを光ピックアップ２

２に供給して、ＤＶＤディスク２０に照射されるレーザ光の出力が所望のレベルとなるように制御される。

【００３１】デコーダ部２７では、ウォーブル信号Ｓwbに基づきディスク上の位置を示すアドレス信号Ｄadを生成して動作制御部４０に供給する。また、リードチャネル部３０では、供給された読出信号ＳRFのアシンメトリ補正及び２値化を行いディジタル信号に変換して、データ信号ＤRFとしてデータ処理部３１と暗号鍵生成部３３に供給する。

【００３２】データ処理部３１では、データ信号ＤRFを８／１６復調すると共にＲＡＭ（Random Access Memory）３２を用いてリードソロモン積符号による誤り訂正処理等も行う。ここで誤り訂正処理がなされたデータ信号は、データ信号ＲＤＳとして暗号処理部３５に供給される。

【００３３】設定信号生成手段である暗号鍵生成部３３では、供給されたデータ信号ＤRFに基づき、再生制限機能を働かせるように設定された再生許可ビットＰＢＰを有しているか否かを判別する。ここで、再生制限機能を働かせるように設定された再生許可ビットＰＢＰを有していると共に再生許可条件も満たしていると判別した場合には、コンテンツ信号を正しく出力可能とする設定信号、すなわち暗号化されているデータ信号ＲＤＳを正しく復号化するための暗号鍵Ｋpを生成して、出力処理手段を構成する暗号処理部３５に供給する。また、再生制限機能が利用されていない場合や再生許可条件を満たしていないときには、従来のディスク装置と同様に暗号鍵Ｋeを暗号処理部１４に供給する。

【００３４】図５は、暗号鍵生成部３３の構成を示しており、暗号鍵生成部３３の鍵情報抽出部３３１では、マスター鍵Ｋmで暗号化されている暗号鍵Ｋe’やＢＣＡ領域に記録されているディスク固有の情報を抽出して鍵生成部３３９に供給する。また、メタデータ抽出部３３２では、コンテンツのメタデータを抽出してメタデータ解析部３３３に供給する。

【００３５】メタデータ解析部３３３では、抽出されたメタデータに基づいて、再生許可ビットＰＢＰや再生条件情報ＰＢＣの検出を行う。ここで、再生許可ビットＰＢＰが検出されて、この再生許可ビットＰＢＰが再生制限機能を働かせるように設定されているときには、スイッチ制御信号ＳＷＣによってスイッチ３３４及びスイッチ３３５をオン状態とする。また、再生許可ビットＰＢＰを有していないとき、あるいは再生許可ビットＰＢＰが再生制限機能を働かせるように設定されていないときには、スイッチ３３４及びスイッチ３３５をオフ状態とする。また、再生条件情報ＰＢＣを有しているときには、スイッチ３３６の可動端子ｃを端子ａ側とすると共に、再生条件情報ＰＢＣを有していないときには、スイッチ３３６の可動端子ｃを端子ｂ側に設定する。さらに、メタデータ解析部３３３では、再生許可ビットＰＢＰや再生条件情報ＰＢＣの検出結果を示す検出信号ＤＴａを動作制御部４０に供給する。

【００３６】スイッチ３３４の一方の端子は再生許可ビット抽出部３３７と接続されると共に、他方の端子は鍵生成部３３９と接続されている。また、再生許可ビット抽出部３３７は、メタデータから再生許可ビットＰＢＰを抽出する。この抽出された再生許可ビットＰＢＰは、スイッチ３３４を介して鍵生成部３３９に供給される。

【００３７】スイッチ３３５の一方の端子はスイッチ３３６の可動端子ｃと接続されると共に、他方の端子は鍵生成部３３９と接続されている。スイッチ３３６の端子ａは再生条件情報抽出部３３８と接続されると共に、端子ｂは後述する通信部４５と接続される。

【００３８】再生条件情報抽出部３３８では、メタデータから再生条件情報ＰＢＣを抽出すると共に、この再生条件情報ＰＢＣで示された再生許可条件を満たすか否かを判別する。ここで、再生許可条件を満たすと判別したときには、コンテンツ信号の再生を許可する許可信号ＥＣを生成してスイッチ３３６，３３５を介し鍵生成部３３９に供給する。また、再生条件情報抽出部３３８では、再生許可条件を満たすと判別したとき、再生条件情報ＰＢＣを鍵生成部３３９に供給しても良い。

【００３９】また、スイッチ３３６に接続された通信部４５を介して外部から再生許可条件を示す条件信号ＥＤが供給されたときには、この条件信号ＥＤをスイッチ３３６，３３５を介して鍵生成部３３９に供給する。

【００４０】鍵生成部３３９では、マスター鍵Ｋmで暗号化されている暗号鍵Ｋe’を復号化して暗号鍵Ｋeを生成する。あるいはディスク固有の情報に基づき暗号鍵Ｋeを生成する。また、再生許可ビットＰＢＰが再生制限機能を働かせるように設定されていると共に、許可信号ＥＣや条件信号ＥＤによって再生が許可されているときには、再生許可ビットＰＢＰに基づく暗号鍵Ｋpbpの生成を行う。さらに、鍵生成部３３９では、暗号鍵Ｋpbpが生成されていないときには、暗号鍵Ｋeを暗号処理部３５に供給すると共に、暗号鍵Ｋpbpが生成されているときには、暗号鍵Ｋeと暗号鍵Ｋpbpから新たな暗号鍵Ｋpを生成して暗号処理部３５に供給する。なお、再生条件情報抽出部３３８から再生条件情報ＰＢＣが供給されたときには、この再生条件情報ＰＢＣに基づく暗号鍵Ｋpbcを生成して、この暗号鍵Ｋpbcと暗号鍵Ｋeと暗号鍵Ｋpbpから新たな暗号鍵Ｋpを生成して暗号処理部３５に供給する。このように、暗号鍵生成部３３では、再生制限機能を利用しているか否かおよび再生許可条件を満たすか否かによって暗号処理部３５に供給する暗号鍵を異なるものとする。

【００４１】暗号処理部３５では、暗号鍵生成部３３から供給された暗号鍵を用いてデータ信号ＲＤＳの復号化を行い、得られた信号をデータ信号ＲＤとして出力制御部３６に供給する。ここで、再生許可ビットＰＢＰを有

しており暗号鍵Kpで暗号化されたコンテンツ信号を再生する際に、暗号鍵生成部３３から暗号処理部３５に暗号鍵Keが供給されたときには、復号化が正しく行われていない信号がデータ信号ＲＤとして暗号処理部３５から出力制御部３６に供給される。また、暗号鍵生成部３３から暗号処理部３５に暗号鍵Kpが供給されたときには、復号化が正しく行われた信号がデータ信号ＲＤとして暗号処理部３５から出力制御部３６に供給される。なお、再生許可ビットＰＢＰを有していないコンテンツ信号の再生では、コンテンツ信号の暗号化が暗号鍵Keを用いて行われているので、暗号処理部３５から正しく復号化された信号が出力制御部３６に供給されることとなる。

【００４２】出力制御部３６では、データ信号ＲＤが正しく復号化が行われた信号であるか否かの判別を検査データ例えばパリティを用いて行い、正しい信号であるときには、この復号化されたデータ信号ＲＤからパリティを除いた信号をコンテンツ出力信号Doutとして出力する。

【００４３】ここで、図３の信号生成部１１には、コンテンツ信号に復号化が正しく完了したか否かを判別可能とする検査データを付加する機能を持たせるものとして、オーディオデータを圧縮して記録するときには、圧縮単位例えばフレーム単位のデータ毎に検査データとして例えば上述のパリティを付加するように設定する。また、リニアＰＣＭのオーディオデータを記録するときにも、オーディオデータを圧縮して記録する場合と同じ単位毎でパリティを付加するように設定すれば、オーディオデータがどのような信号であるかに係らず図３に示す信号生成部１１や図６の出力制御部３６を共用できる。

【００４４】図６は、出力制御部３６の構成を示している。データ信号ＲＤは、パリティ分離部３６１に供給されて、コンテンツ信号に付加されているパリティＰの分離が行われる。このパリティＰは、上述したようにコンテンツ信号に対して所定単位毎に付加するように設定されているので、パリティ分離部３６１では、データ信号ＲＤからパリティＰに相当するデータを分離して比較値算出部３６２に供給する。また、パリティＰに相当するデータが除かれたデータはスイッチ３６４に供給する。ここで、暗号処理部３５で正しい暗号鍵を用いた復号化が行われたときには、パリティ分離部３６１では、正しくパリティＰが分離される。また、暗号処理部３５で正しくない暗号鍵を用いた復号化が行われたときには、パリティ分離部３６１で分離されたデータは、所定単位毎に付加したパリティＰとは異なったものとなる。

【００４５】比較値算出部３６２では、あるデータが与えられた時、このデータに対応する数値を求めることができる信号処理関数を用いて比較値ＲＱを算出する。例えばハッシュ関数を予め設定しておくものとして、この関数にパリティ分離部３６１で分離されたデータを代入することで比較値ＲＱを算出して判定部３６３に供給する。

【００４６】判定部３６３には、後述する動作制御部４０から正しいパリティＰを用いて求めた初期値ＲＳが供給されており、この初期値ＲＳと比較値算出部３６２から供給された比較値ＲＱが等しいときには、スイッチ制御信号ＳＷＤによってスイッチ３６４をオン状態とする。

【００４７】すなわち、出力制御部３６では、パリティ分離部３６１でパリティとして分離されたデータが、コンテンツの信号に付加したパリティと等しい場合に、暗号処理部３５で正しい暗号鍵を用いた復号化が行われたものと判別する。このとき、パリティが除かれた信号がコンテンツ出力信号Doutとして出力制御部３６から出力される。

【００４８】また、初期値ＲＳと比較値ＲＱが等しくないときには、暗号処理部３５で正しくない暗号鍵を用いた復号化が行われたと判別して、スイッチ３６４をオフ状態とすることにより、正しくないコンテンツ信号が出力制御部３６から出力されてしまうことを防止する。さらに、初期値ＲＳと比較値ＲＱが等しくないことを動作制御部４０に通知して、動作制御部４０によって後述する表示部４２にコンテンツ信号の再生が制限されていることを表示する。なお、コンテンツ信号の再生が制限されていることは、音声等を利用して通知するものとしても良い。このように、コンテンツ信号の再生が制限されていることを通知することで、ディスク装置の異常によってコンテンツ信号の再生が行われない場合との区別を容易に判断できる。

【００４９】次に、コンテンツ信号を記録する場合、コンテンツ信号Ｄinが供給されると、この信号Ｄinは入力処理部３８に供給される。入力処理部３８では、上述したように、コンテンツ信号Ｄinに対して所定単位毎に検査データであるパリティＰを付加する。また、動作制御部４０から再生許可ビットＰＢＰや再生条件情報ＰＢＣが供給されたときには、これらの信号をコンテンツ信号に付加して、ＤＶＤディスク２０に記録するコンテンツ信号WDとして暗号処理部３５に供給する。

【００５０】暗号鍵生成部３３の鍵生成部３３９には、再生許可ビットＰＢＰや再生条件情報ＰＢＣ等が動作制御部４０から供給されて、上述のＣＰＲＭの暗号方式で示したように、ディスク固有の情報を利用した暗号鍵Keとトラック単位毎の暗号鍵Ktや再生許可ビットＰＢＰ、再生条件情報ＰＢＣを用いて新たな暗号鍵Kpを生成して暗号処理部３５に供給する。

【００５１】暗号処理部３５では、供給された暗号鍵Kpを用いてコンテンツ信号WDの暗号化を行い、コンテンツ信号ＷＤＳとしてデータ処理部３１に供給する。データ処理部３１では、データ信号DRFからデータ信号ＲＤＳを生成する処理とは逆の処理を行い、コンテンツ信

号ＷＤＳから記録信号Ｄｗを生成して記録駆動部３９に供給する。記録駆動部３９では、記録信号Ｄｗに基づきレーザ駆動信号ＬＤを生成して光ピックアップ２２に供給する。光ピックアップ２２では、このレーザ駆動信号によってレーザ光の出力を制御することにより、コンテンツの信号をＤＶＤディスク２０に記録する。

【００５２】動作制御部４０には、操作部４１や表示部４２が接続されており、操作部４１のからの操作信号ＰＳに基づき制御信号ＣＴを生成して各部に供給することにより、操作部４１の操作に応じた動作を行わせる。また、表示部４２に表示信号ＰＤを供給して、ＤＶＤディスク２０に記録されている情報の表示やディスク装置の動作状態等を表示する。また、動作制御部４０では、コンテンツ信号の暗号化や復号化及び暗号鍵の生成等の動作、及び通信部４５を介した再生許可条件の入手動作、初期値ＲＳを出力制御部３６に供給して正しいコンテンツ信号のみを出力させる動作等の制御を行う。

【００５３】通信部４５では、ＤＶＤディスク２０やディスク装置が再生許可条件を有していないときに、通信回線を介して再生許可条件の入手を行う。また、通信回線を介して種々の情報の通信を行う。さらに、ディスク装置は、不揮発性メモリ４６を有しており、この不揮発性メモリ４６に再生許可条件やコンテンツ信号の再生に関する情報を保持することが可能とされている。

【００５４】次に、再生許可ビットＰＢＰや再生条件情報ＰＢＣを用いたコンテンツ信号の再生動作について説明する。まず、再生制限機能を働かせるように設定された再生許可ビットＰＢＰを有していると共に、再生条件情報ＰＢＣを有していない場合の動作について説明する。この場合には、再生条件情報ＰＢＣを入手する処理を行い、再生許可条件を満たすか否かを判別し、再生許可条件を満たすと判別されたときに再生許可ビットＰＢＰに基づく暗号鍵Ｋpbpを生成して、この暗号鍵Ｋpbpを用いて正しい暗号鍵Ｋpを生成する。

【００５５】例えば、コンテンツ信号の再生時に、通信部４５を介してコンテンツ提供者側あるいはコンテンツの配布を管理するコンテンツ管理者側に対し再生許可条件の要求を行う。コンテンツ提供者あるいはコンテンツ管理者は、コンテンツ信号再生装置と通信を行い、いずれの装置でどのようなコンテンツ信号の再生が行われるかを判別して、コンテンツ信号の使用状況を管理する。また、要求のあったディスク装置側に供給する再生許可条件として、コンテンツ信号の再生を許可する信号を条件信号ＥＤとして供給する。この供給された条件信号ＥＤは、スイッチ３３６及びスイッチ３３５を介して鍵生成部３３９に供給される。鍵生成部３３９では、条件信号ＥＤによってコンテンツ信号の再生が許可されていることから、再生許可ビットＰＢＰに基づく暗号鍵Ｋpbpを生成すると共に、この暗号鍵Ｋeと暗号鍵Ｋpbpを用いて暗号鍵Ｋpを生成して暗号処理部３５に供給する。このため、暗号鍵Ｋpを用いてコンテンツの復号化を正しく行うことができる。また、コンテンツ提供者あるいはコンテンツ管理者はディスクに再生許可ビットＰＢＰを設けておくことで、ディスク装置側でのコンテンツ信号の再生を管理することが可能となり、コンテンツ信号の再生に対して課金することができる。なお、コンテンツの使用料の徴収は電話料金に加算しても良く、また別個に請求するなど種々の方法が考えられる。

【００５６】また、再生条件情報ＰＢＣを有していない場合には、再生条件情報ＰＢＣを入手する処理が行われるので、例えば通信部４５を介して再生条件情報ＰＢＣを供給することにより、コンテンツ信号を流通させてからでも、再生許可条件の設定や変更を自由に行うことが可能となり、コンテンツ信号の再生制限動作の自由度を高めることができる。

【００５７】さらに、暗号鍵生成部３３では、コンテンツ信号に再生制限機能を働かせるように設定された再生許可ビットＰＢＰが付加されている場合、自動的にコンテンツ信号の再生を許可するものとし、コンテンツ信号の利用状態を示す利用情報、例えばコンテンツ信号の再生回数や再生時間をコンテンツ毎に改竄できないように不揮発性メモリ４６に記憶するものとしても良い。ここで、コンテンツ提供者あるいはコンテンツ管理者は、不揮発性メモリ４６に記憶されている利用情報を所定期間経過毎に通信部４５を介して読み出すものとすれば、上述の場合と同様にコンテンツ信号の再生に対して課金することができる。

【００５８】また、使用料を先払いして、支払った使用料分だけコンテンツの再生を可能とすることもできる。例えばコンテンツ信号の再生可能回数が購入料金に応じて設定されているプリペードカードを設けると共に、このプリペードカードの情報の読み取りや更新を行うことができるカード処理部（図示せず）をディスク装置に設ける。ここで、再生制限機能を働かせるように設定された再生許可ビットＰＢＰを有しているコンテンツ信号を再生する場合、プリペードカードを購入してカード処理部（図示せず）に装着させる。カード処理部では、コンテンツ信号の再生回数毎に、プリペードカードの使用可能残り回数情報を順次更新するものとし、使用可能回数が無くなったときには、暗号鍵生成部３３において正しい暗号鍵Ｋpの生成を禁止することで、コンテンツ信号の再生を購入料金分だけに制限することもできる。

【００５９】次に、再生制限機能を働かせるように設定された再生許可ビットＰＢＰと再生条件情報ＰＢＣを有している場合の動作について説明する。ここで、再生条件情報抽出部３３８では、コンテンツ信号から再生条件情報ＰＢＣを抽出して、再生許可条件を満たすか否かを判別するものとし、再生許可条件を満たすと判別したときには許可信号ＥＣを鍵生成部３３９に供給して、鍵生成部３３９で正しい暗号鍵Ｋpの生成を行う。また、再

生許可条件を満たすと判別されないときには鍵生成部３３９への許可信号ＥＣの供給を停止して、鍵生成部３３９によって正しい暗号鍵Kpが生成されることを禁止する。

【００６０】例えば、再生条件情報ＰＢＣで再生回数が示される場合、ディスク装置では、再生制限機能を働かせるように設定された再生許可ビットＰＢＰを有したコンテンツ信号の再生回数情報を、ディスク固有の情報やディスクのタイトル固有の情報と対応付けて不揮発性メモリ４６に保持させる。ここで、再生制限機能を働かせるように設定された再生許可ビットＰＢＰを有するコンテンツ信号の再生が行われたとき、不揮発性メモリ４６に保持されている再生回数が再生条件情報ＰＢＣで示された再生回数に達していないときには、許可信号ＥＣを鍵生成部３３９に供給して正しい暗号鍵Kpを暗号処理部３５に供給させる。また、不揮発性メモリ４６に記憶されている再生回数に「１」を加算して、再生回数情報を更新する。その後、再生回数が再生条件情報ＰＢＣで示された回数に達したときには、鍵生成部３３９への許可信号ＥＣの供給を停止して、暗号処理部３５に正しい暗号鍵Kpが供給されることを禁止する。

【００６１】このように、再生条件情報ＰＢＣで再生回数を指定することにより、コンテンツの再生回数が指定された再生回数で制限されるので、再生回数を制限した状態でプレビューサービス等を容易に行うことができる。

【００６２】また、記録可能な領域を有するディスクを用いる場合には、この領域に再生回数を示す情報を書き込むものとしても良い。この場合には、不揮発性メモリ４６に再生回数を示す情報を記憶させておかなくとも、コンテンツの再生回数をコンテンツの再生条件情報ＰＢＣで示された回数に制限できる。

【００６３】さらに、再生条件情報ＰＢＣは、再生回数だけでなく再生可能期間を設定するものとしても良い。例えば、再生条件情報ＰＢＣでは、使用開始から所定日数だけコンテンツ信号の再生を許可するものとすると共に、ディスク装置では、正しい暦情報及び時刻情報を入手して、この正しい暦情報及び時刻情報を用いて動作を行うものとする。

【００６４】ここで、コンテンツ信号の再生が最初に行われたときには、正しい暦情報及び時刻情報を用いて、ディスク装置の不揮発性メモリ４６やディスクの記録可能領域にコンテンツ信号の利用開始時を登録する。その後、コンテンツ信号の再生毎に、登録されている利用開始時から再生条件情報ＰＢＣで示された期間が経過しているか否かを判別して、再生条件情報ＰＢＣで示された期間が経過したとき鍵生成部３３９への許可信号ＥＣの供給を停止する。すなわち、再生条件情報ＰＢＣで示された期間までは、正しい暗号鍵Kpを生成して暗号処理部３５に供給する。その後、期間が経過したときには、

正しい暗号鍵Kpの生成を禁止して暗号処理部３５で復号化が正しく行われることを防止することにより、コンテンツ信号の使用を所定期間内に制限することができる。

【００６５】また、上述の実施の形態では、ＤＶＤディスクに記録されているコンテンツ信号を再生する場合について説明したが、記録媒体はＤＶＤディスクに限られるものではなく、他の光ディスクあるいは磁気を利用した記録媒体や半導体素子を用いて構成された記録媒体であっても良い。

【００６６】さらに、再生制限を行うコンテンツ信号は、記録媒体に記録されているコンテンツ信号だけでなく、無線あるいは有線の伝送路を介して配信されるコンテンツ信号であっても良い。この場合にも、コンテンツ信号にコンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号や再生制限機能を働かせたときにコンテンツ信号の再生許可条件を示す条件信号を付加することで、上述の場合と同様にコンテンツ信号の再生を制限することができる。この場合のコンテンツ信号再生装置を図７に示す。なお、図７において、図４と対応する部分については同一符号を付し、詳細な説明は省略する。

【００６７】図７において、通信部４５を介して供給されたコンテンツ信号ＣＳは、ハード・ディスク装置や半導体メモリ等を用いて構成されたコンテンツ記憶部５０に蓄積される。コンテンツ信号の再生時には、コンテンツ記憶部５０から所望のコンテンツ信号ＣＳが読み出されて信号処理部５１や暗号鍵生成部３３に供給される。

【００６８】信号処理部５１では、コンテンツ信号ＣＳがデータ圧縮されているときに伸長処理等を行い、伸長処理後の信号ＲＤＳを暗号処理部３５に供給する。暗号鍵生成部３３では、コンテンツ記憶部５０から読み出したコンテンツ信号ＣＳあるいは信号処理部５１から出力された信号ＲＤＳが、再生許可ビットＰＢＰや再生条件情報ＰＢＣを有しているか否かを検出する。さらに、検出結果及び再生許可条件を満たすか否かを判別して暗号鍵の生成を行うことで、上述の場合と同様に出力制御部３６からのコンテンツ信号の出力を制御して、配信されたコンテンツ信号ＣＳに対しても再生制限を行うことができる。

【００６９】また、上述の実施の形態では、コピー制限機能を高めるために暗号化されたコンテンツ信号に対して再生制限を行い、暗号化されたコンテンツ信号の復号化で用いる暗号鍵の生成や正しく復号化が行われたか否かによって、正しいコンテンツ信号の出力を制限したが、コンテンツ信号は暗号化された信号に限られるものではない。例えば、暗号化されていないコンテンツ信号に対しては、再生制限機能が有効とされて再生許可条件が満たされている場合にのみ出力を行うものとすることでも、コンテンツ信号の再生を制限できる。

【００７０】

【発明の効果】この発明によれば、コンテンツ信号に、このコンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号が付加されると共に、このコンテンツ信号の再生時には制御信号が付加されているか否かが検出される。このため、制御信号によって再生制限機能を働かせることによって、コンテンツ信号の再生を制限することができる。

【００７１】また、再生制限機能を働かせたときにコンテンツ信号の再生許可条件を示す条件信号が付加されると共に、このコンテンツ信号の再生時には再生許可条件を満たすか否かが判別されて、再生条件を満たすときにコンテンツ信号の再生が行われる。このため、再生許可条件を変更することで、コンテンツ信号の再生の制限を自由に変更することができる。

【００７２】また、再生制限機能を働かせたとき、コンテンツ信号に再生許可条件を示す条件信号が付加されていないときには、コンテンツ信号の再生時に、再生許可条件が入手されて、この入手された再生許可条件を満たすときにコンテンツ信号の再生が行われる。このため、再生許可条件を付加することができないようなコンテンツ信号に対してもコンテンツ信号の再生を制限できる。また、コンテンツ信号を流通させた後からでも、自由に再生許可条件を設定することができるので、様々な再生制御動作を行うことができる。さらに、コンテンツ信号の再生を制限するために制御信号を付加するだけ良いことから、コンテンツ信号の再生を制限できるように既存の信号フォーマットを容易に対応させることができる。

【００７３】また、コンテンツ信号は、再生制限機能を働かせるか否かを示す制御信号と予め設定された暗号鍵、あるいは制御信号と暗号鍵と再生許可条件を示す条件信号を用いて生成された暗号鍵によって暗号化されると共に、このコンテンツ信号の再生時には、再生許可条件を満たすときに、制御信号や予め設定された暗号鍵及び条件信号を用いて暗号化に用いた暗号鍵が生成されて、この生成された暗号鍵で復号化が行われる。このため、既存の暗号化方式を用いて暗号鍵の生成方法を変更するだけで、暗号化されたコンテンツ信号に対しても簡単にコンテンツ信号の再生を制御することができる。また、制御信号や条件信号を用いて暗号鍵が生成されるので、制御信号や条件信号が改竄されたときには正しい暗号鍵を得ることができないと共に、制御信号や条件信号をそのまま用いて復号化を行うものでもないことから、制御信号や条件信号は暗号化しなくとも良い。すなわち、暗号化する信号が増加するものでないことから、従来のコンテンツ信号の暗号化におけるフォーマットを大きく変更することなく利用できる。

【００７４】さらに、コンテンツ信号の再生が制限されたときには、表示や音声によって通知されるので、コンテンツ信号の出力が行われない原因が再生装置の異常であるか再生制限が行われたことによるものか容易に判別できる。

【図面の簡単な説明】

【図１】コンテンツの構造を示す図である。

【図２】ＤＶＤのディスク構成の一例を示す図である。

【図３】コンテンツ信号生成装置の構成を示す図である。

【図４】ディスク装置の構成を示す図である。

【図５】暗号鍵生成部の構成を示す図である。

【図６】出力制御部の構成を示す図である。

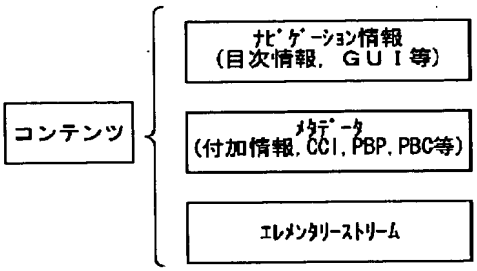
【図７】配信されたコンテンツ信号の再生装置の構成を示す図である。

【符号の説明】

１１・・・信号生成部、１２・・・記憶装置、１３・・・信号生成制御部、１４・・・暗号処理部、１５・・・暗号鍵生成部、１６・・・信号変換部、２０・・・ＤＶＤディスク、２１・・・スピンドルモータ部、２２・・・光ピックアップ、２３・・・ＲＦアンプ部、２６・・・サーボ制御部、２７・・・デコーダ部、２８・・・ドライバ、２９・・・スレッド部、３０・・・リードチャネル部、３１・・・データ処理部、３３・・・暗号鍵生成部、３５・・・暗号処理部、３６・・・出力制御部、３８・・・入力処理部、３９・・・記録駆動部、４０・・・動作制御部、４１・・・操作部、４２・・・表示部、４５・・・通信部、４６・・・不揮発性メモリ、５０・・・コンテンツ記憶部、５１・・・信号処理部、３３１・・・鍵情報抽出部、３３２・・・メタデータ抽出部、３３３・・・メタデータ解析部、３３４，３３５，３３６，３６４・・・スイッチ、３３７・・・再生許可ビット抽出部、３３８・・・再生条件情報抽出部、３３９・・・鍵生成部、３６１・・・パリティ分離部、３６２・・・比較値算出部、３６３・・・判定部

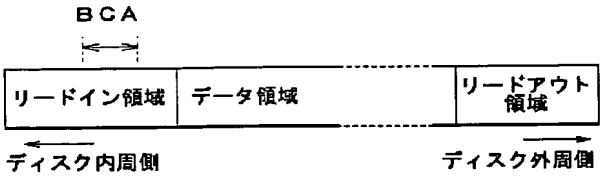
【図１】

コンテンツの構造



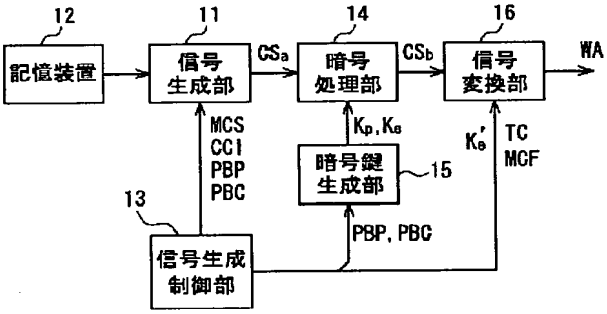
【図２】

ＤＶＤのディスク構成



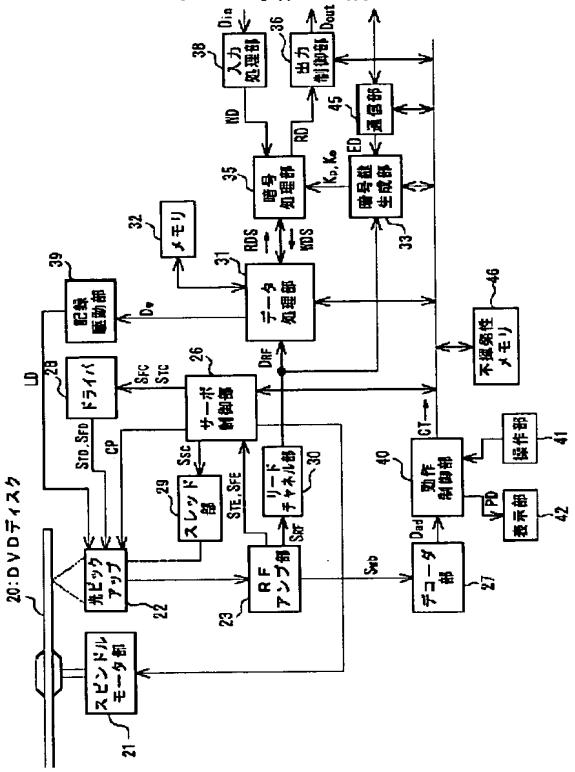
【図３】

コンテンツ信号生成装置



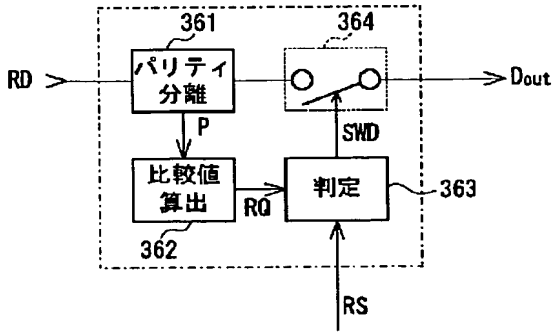
【図４】

ディスク装置の構成



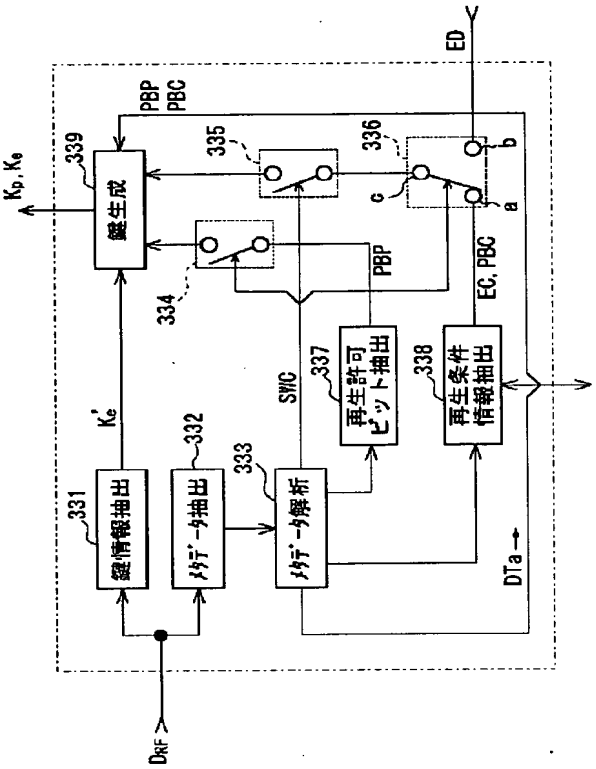
【図６】

出力制御部の構成



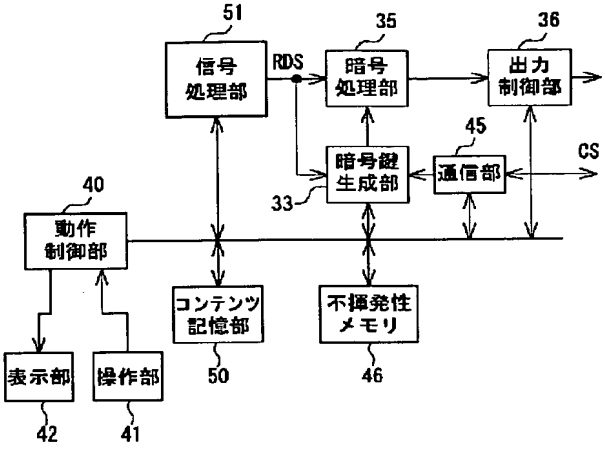
【図５】

暗号鍵生成部の構成



【図７】

配信されたコンテンツ信号の再生装置の構成



フロントページの続き

Ｆターム(参考) 5C053 FA13 FA24 GA11 GB37 JA01
JA21 KA01 KA08 KA16 KA24
LA14
5D044 AB05 AB07 BC03 CC06 DE50
DE53 EF05 FG18 GK08 GK17
HL08 HL11
5J104 AA16 EA02 EA04 EA22 NA02
PA14

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- [x] BLACK BORDERS
- [ ] IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- [x] FADED TEXT OR DRAWING
- [ ] BLURED OR ILLEGIBLE TEXT OR DRAWING
- [ ] SKEWED/SLANTED IMAGES
- [x] COLORED OR BLACK AND WHITE PHOTOGRAPHS
- [ ] GRAY SCALE DOCUMENTS
- [x] LINES OR MARKS ON ORIGINAL DOCUMENT
- [ ] REPERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- [ ] OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning documents *will not* correct images problems checked, please do not report the problems to the IFW Image Problem Mailbox